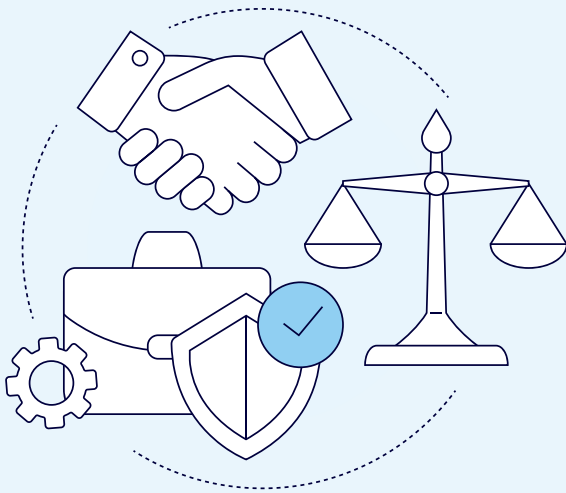




Law Firm Vendor Security Evaluation Workbook

Purpose: This workbook is designed to help distinguish between operational security maturity and marketing language when evaluating technology vendors.

Most law firms are not trying to become security experts. The challenge is determining whether a vendor demonstrates real operational maturity or simply presents a polished story.

We are not looking for perfection. We are looking for transparency, accountability, and evidence of how security is managed in practice. Mature vendors can speak candidly about ownership, timelines, lessons learned, and the realities of operating a secure environment. The depth and specificity of those conversations often reveal more than any individual answer.

How to Use This Worksheet

Ask each question as written.

Listen for specifics rather than promises.

Score each response from 1-5.

Record examples and observations.

Review the total score and red flags before making a decision.

SCORE	ASSESSMENT
5	Highly specific answer with evidence and ownership
4	Good answer with clear processes
3	Adequate answer with gaps
2	Mostly marketing language
1	Cannot answer or avoids question

Question 1

Tell Me About Your Most Significant Security Incident or Service Outage

Every organization experiences incidents. The goal is not to find a vendor with a perfect history. The goal is to understand how they respond when things go wrong. Organizations with mature security programs can explain what happened, what they learned, and what changed afterward.

STRONG INDICATORS

- Explains a specific incident
- Describes root cause
- Discusses lessons learned
- Details corrective actions
- Demonstrates transparency

RED FLAGS

- Claims no incidents have occurred
- Refuses to discuss incidents
- Redirects to certifications
- No examples provided
- No lessons learned

Example of a strong answer: "In 2024, a configuration error caused a service interruption. We identified the issue quickly, implemented new monitoring controls, revised change management procedures, and added validation checks."

SCORE

____/5

NOTES

Question 2

How Do You Validate That Your Security Controls Actually Work?

Security controls are only valuable if they are tested. This question separates organizations that actively validate their controls from organizations that rely primarily on certifications or policy documents.

STRONG INDICATORS

- Annual independent penetration testing
- Recent SOC 2 Type II report
- Vulnerability scanning program
- Defined remediation process
- Willingness to share evidence

RED FLAGS

- We are SOC 2 compliant with no further explanation
- No testing cadence
- Cannot explain remediation process
- Relies entirely on certifications
- No supporting evidence

Example of a strong answer: "We complete annual third-party penetration tests, perform regular vulnerability scanning, maintain a SOC 2 Type II report, and track remediation through a formal governance process."

SCORE

____/5

NOTES

Question 3

Who Owns Security Within Your Organization?

Security requires ownership. If nobody clearly owns security, accountability becomes difficult and important risks often go unresolved.

STRONG INDICATORS

- Named security leader
- Clear reporting structure
- Defined governance process
- Security SMEs available
- Security involved in decisions

RED FLAGS

- No single person has accountability
- No dedicated security staff
- Unclear ownership
- No knowledgeable personnel
- Salesperson answers everything

Example of a strong answer: "Our Director of Security owns the program and reports to executive leadership. Security reviews major releases and vendor relationships."

SCORE

____/5

NOTES

Question 4

How Do You Protect Access to Customer Data?

Most breaches ultimately involve access. Strong identity and access management practices reduce the likelihood that an attacker can reach sensitive customer information.

STRONG INDICATORS

- MFA required for all employees
- Enhanced controls for privileged users
- Regular access reviews
- Formal onboarding/offboarding
- Least-privilege model

RED FLAGS

- MFA optional
- No access review process
- Cannot explain access removal
- Generic statements
- No distinction for privileged access

Example of a strong answer: "MFA is mandatory for all employees. Administrative access requires additional controls. Access reviews occur quarterly."

SCORE

____/5

NOTES

Question 5

How and When Will You Communicate With Customers During a Security Event?

The quality of a vendor communication process often determines whether an incident becomes manageable or chaotic. Mature vendors have defined timelines and escalation procedures.

STRONG INDICATORS

- Defined notification timeline
- Contractual commitments
- Established communication process
- Regular updates
- Clear escalation procedures

RED FLAGS

- As appropriate
- No documented process
- No contractual commitments
- Cannot explain procedures
- Vague timelines

Example of a strong answer: "Customers are notified within 24 hours of confirming an incident affecting their data. Updates continue throughout remediation."

SCORE

____/5

NOTES

Final Evaluation

As questions become more challenging, mature organizations respond with greater specificity, including owners, timelines, processes, evidence, and real-world examples. Tally up your scores to each question, then check the red flags.

RED FLAG CHECKLIST

- ☐ Claims no incidents have occurred
- ☐ Cannot identify who owns security
- ☐ Relies entirely on certifications
- ☐ Refuses to discuss testing
- ☐ Cannot explain access controls
- ☐ No breach notification timeline
- ☐ Claims SOC 2 compliance with no further explanation

TALLY YOUR SCORE

Question 1: _____

Question 2: _____

Question 3: _____

Question 4: _____

Question 5: _____

Total Score: _____

About SurePoint® Technologies

SurePoint drives Firm Performance by helping mid-sized law firms operate efficiently, compete effectively, and grow with confidence. Powered by a connected legal technology ecosystem, its configurable Practice, Finance, and Growth solutions streamline operations, so legal professionals can focus on what matters most: serving clients and leading with impact. **Learn more about SurePoint's security:** surepoint.com/security/